4 比特 S 盒输入及输出低次代数关系分析 *

程月单 [a]，韦永壮 [b, c†]，叶　涛 [a]

(桂林电子科技大学 a.广西无线宽带通信与信号处理重点实验室; b.广西密码学与信息安全重点实验室; c.广西高校云计算与复杂系统重点实验，广西　桂林　541004)

摘　要：随着 4 比特 S 盒在轻量级密码算法中的广泛应用，如何捕获这些 4 比特 S 盒其输入及输出的代数关系成为了目前的研究热点之一。根据 S 盒的输入输出关系，提出了 n 比特 S 盒的非线性回路代数关系的通用求解算法。针对 4 比特 S 盒设计了高效的非线性回路代数关系求解算法，并对国际公认的 16 类最优 4 比特 S 盒及多个著名的轻量级密码算法中的 S 盒进行了测试分析。同时，还对上述轻量级密码算法中 S 盒所属等价类进行了检测。研究结果表明：16 类 S 盒代表元中只有 3 类不存在二次回路代数关系；同属等价类 S 盒可能会有不同的二次回路代数关系；MANTIS，PRIDE，Marvin 等轻量级算法的 S 盒存在多个二次回路代数关系。即这些包含低次回路代数关系的 S 盒存在潜在的安全缺陷。

关键词：4 比特 S 盒；轻量级密码算法；代数关系；非线性方程

中图分类号：TP309.7　　doi: 10.19734/j.issn.1001-3695.2018.08.0658

New analysis of low degree algebraic relation between input and output of 4-bit s-boxes

Cheng Yuedan[a], Wei Yongzhuang[b, c†], Ye Tao[a]

(*a. Guangxi Key Laboratory of Wireless Wideband Communication & Signal Processing, b. Guangxi Key Laboratory of Cryptography & Information Security, c. Guangxi Colleges & Universities Key Laboratory of Cloud Computing & Complex Systems, Guilin University of Electronic Technology, Guilin Guangxi* 541004, *China*)

Abstract: Currently, with the extensive use of the 4-bit S-Boxes in lightweight encryption algorithms, it appears to be an important issue to look for the algebraic relationships between their inputs and outputs. This paper proposed a general algorithm for calculating the nonlinear loop algebraic relationships by using the low algebraic relationships between input and output of S-Box. Moreover, it checked algebraic relationships of both the well-known optimal 4-bit S-Boxes and the S-boxes used in some famous lightweight encryption algorithms. The results shown that only 3 classes of 16 categories of optimal 4-bit S-Boxes had square loop algebraic relationships. In particular, the S-Boxes belonging to the same equivalence class may possess different square loop algebraic relationships. Furthermore, the S-Boxes of some lightweight cryptographic algorithms (e. g. , MANTIS, PRIDE, and Marvin) had many square loop algebraic relationships. There exists potential security flaws of these S-boxes which possess low degree algebraic relationships.

Key words: 4-bit S-box; lightweight algorithms; algebraic relationship; affine equivalence

0　引言

1974 年，Feistel 在文献[1]中首次提出密码 S 盒的概念。随着数据加密标准(DES)[2]的广泛应用，S 盒已经成为对称密码算法设计的关键。S 盒以 4 比特和 8 比特最为常见，例如，AES[3]中使用了 8 比特 S 盒。SERPENT[5]和 NOEKEON[6]则使用了 4 比特 S 盒。注意到，在硬件实现时，8 比特 S 盒往往会消耗更多硬件电路。因此，为了减少硬件面积消耗，提高数据处理速度，4 比特 S 盒在资源受限的轻量级密码算法的设计中得到了广泛应用[7]，如分组密码 PRESENT[8]，PRINT[9]，LED[10]，LBlock[11]，PRINCE[12]，SIMON[13]，SPECK[13]，RECTANGLE[14]，PRIDE[15]，MANTIS[16]，SKINNY[16]，GIFT[17]，GRANULE[18]，Marvin[19]等，哈希函数 PHONTON[20]，SPONGENT[21]等。

S 盒的安全性指标有差分均匀性、(非)线性度、代数次数及项数分布、代数免疫阶等[22]，但目前对 S 盒的研究主要集中于差分均匀性和非线性度[23]。针对 4 比特 S 盒的这两种代数关系，2007 年，Leander 等人[4]提出最优 S 盒的概念，并将所有 4 比特最优 S 盒分为 16 类。2011 年，Markku 在文献[24]中展示了所有 4 比特 S 盒的置换等价类。同年，Ullrich 等人[25]将便于硬件实现的 4 比特 S 盒分为 302 个仿射等价类。在 FSE2015 会议上，Zhang 等人[26]将所有 4 比特最优 S 盒划分为 183 类。2016 年，Cheng 等人[7]提出了一种 4 比特双射 S 盒的置换等价类优化的搜索算法。2016 年亚洲密码会议上，Todo 等人[27]针对一些轻量级密码算法密钥编排简单的特点提出了非线性不变子攻击。2017 年，Beierle 等人[29]提出了通过选择合适的轮常量来抵抗非线性不变子的方法。2018 年，Beyne 将分组密码的非线性不变子作为相关矩阵的特征

收稿日期：2018-08-30；**修回日期：**2018-11-14　**基金项目：**国家自然科学基金资助项目（61572148，61872103）；广西研究生教育创新计划资助项目（YCBZ2018051）；桂林电子科技大学研究生优秀学位论文培育资助项目（16YJPYSS12）；桂林电子科技大学研究生教育创新计划资助项目（2018YJCX45）

作者简介：程月单（1992-），女，河北保定人，硕士研究生，主要研究方向为分组密码非线性部件分析；韦永壮（1976-），男（壮族）（通信作者），广西田阳人，教授，博士，主要研究方向为对称密码算法设计与分析、密码芯片侧信道分析与防护方法（walker_wyz@guet.edu.cn）；叶涛（1991-），男，黑龙江伊春人，博士研究生，主要研究方向为分组密码的设计与分析.

向量，并和积分攻击相结合，提出了新的非线性不变子的分析方法[31]。2018 年，Wei 等人[30]提出了广义非线性不变子攻击方法。注意到，文献[30]提出了密码算法的非线性回路方程的概念，但未给出非线性回路方程的快速求解算法。特别地，随着新攻击方法的出现，S 盒是否存在新的安全缺陷等问题，仍有待进一步解决。

本文利用 S 盒的输入输出关系，将非线性回路代数关系作为 S 盒安全性新指标，给出了 4 比特 S 盒非线性回路代数关系的快速求解算法。针对 16 类最优 4 比特 S 盒及多个著名轻量级密码算法 4 比特 S 盒，进行了输入输出的二次回路代数关系测试，并根据仿射等价关系，对被测试 S 盒进行了分类。结果表明：16 类 S 盒代表元只有 3 类不存在二次回路代数关系；大部分轻量级 S 盒存在二次回路代数关系，如近两年提出的 MANTIS，PRIDE，Marvin 等算法的 S 盒均存在二次回路代数关系，这表明实际算法可能存在潜在的安全隐患。

1 预备知识

香农在文献[32]中指出，构建安全的分组密码需具备数据混淆和扩散的能力。在大多数情况下，扩散通过一系列线性操作对状态位混合来实现，而混淆是通过 S 盒并行操作部分状态（通常是字节）来实现的。由此，S 盒的密码学性质对密码的安全性而言意义重大。S 盒经典的安全性指标主要包含非线性度[33,34]和差分均匀性[35]，它们分别是度量算法抵御线性攻击[36]和差分攻击[37]的重要指标。

1.1 类最优 4 比特 S 盒

2007 年，Leander 等人[4]首次定义了 4 比特最优 S 盒，即非线性度和差分均匀性同时达到临界值 4 的双射 S 盒。

定义 1[4] 4 比特 S 盒 S_1， $S_2:F_2^4\rightarrow F_2^4$，若存在 4 阶可逆矩阵 A， $B\in GL(4,F_2)$ 4 比特向量 c， $d\in F_2^4$，使得等式 $S_1(x)=B\bullet(S_2(A\bullet x\oplus c))\oplus d$ 成立，则称 S_1， S_2 仿射等价，记为 $S_1\sim S_2$。 S_1 属于 S_2 的线性等价集合， $S_1\in LE(S_2)$ [24]。

定义 2[4] 已知任意 n 元布尔函数 $f:F_2^n\rightarrow F_2$ 均可用多元多项式形式唯一表示，即

$$f(x)=f(x_1,x_2,\cdots,x_n)=\sum_{u\in F_2^n}C_u x_1^{u_1}x_2^{u_2}\cdots x_n^{u_n}$$

其中: $C_u\in F_2$， $u=(u_1,u_2,\cdots,u_n)$。 $f(x)$ 如上形式一般称为布尔函数的代数正规型（ANF)，它的代数次数 $\deg(f)$ 为非零系数 C_u 对应向量 u 的最大汉明重：

$$\deg(f)=\max_{C_u\neq 0,u\in F_2^n} w(u)$$

此外，由文献[38,39]可知，S 盒仿射等价可以看成对分组密码的线性层作相应改变，S 盒的代数次数、差分均匀性、非线性度在仿射等价下均无变化，是仿射等价的不变量。特别地，若仿射等价中 S_2 为最优 4 比特 S 盒，则 S_1 为相同等价类最优 4 比特 S 盒。Leander 等人[4]通过限定最优 4 比特 S 盒 $S(i)=i(i=0,1,2,4,8)$ 的方法，共找到 16 类最优 4 比特 S 盒的代表元，如表 1 所示。

值得注意的是，对 16 类最优 4 比特 S 盒的代数次数进行分析发现：对于所有的矢量 $p\in F_2^n(p\neq 0)$，存在 8 个非等价最优 S 盒满足 $\deg(S_p)=3$ (详见表 2)。

2 S 盒的非线性回路代数关系

2.1 非线性回路代数关系原理

本节通过分析比较 S 盒的输入输出关系，提出了 S 盒的非线性回路代数关系的快速搜索算法，发现了 S 盒新的代数性质。

表 1 16 类最优 4 比特 S 盒代表元

Table 1 Representatives for all 16 classes of optimal 4 bit S-boxes

S 盒等价类	代表元	S 盒等价类	代表元
G_0	0,1,2,13,4,7,15,6,8,11,14,9,3,14,10,5	G_8	0,1,2,13,4,7,15,6,8,14,9,5,10,11,3,12
G_1	0,1,2,13,4,7,15,6,8,11,14,3,5,9,10,12	G_9	0,1,2,13,4,7,15,6,8,14,11,3,5,9,10,12
G_2	0,1,2,13,4,7,15,6,8,11,14,3,10,12,5,9	G_{10}	0,1,2,13,4,7,15,6,8,14,11,5,10,9,3,12
G_3	0,1,2,13,4,7,15,6,8,12,5,3,10,14,11,9	G_{11}	0,1,2,13,4,7,15,6,8,14,11,10,5,9,12,3
G_4	0,1,2,13,4,7,15,6,8,12,9,11,10,14,5,3	G_{12}	0,1,2,13,4,7,15,6,8,14,11,10,9,3,12,5
G_5	0,1,2,13,4,7,15,6,8,12,11,9,10,14,3,5	G_{13}	0,1,2,13,4,7,15,6,8,14,12,9,5,11,10,3
G_6	0,1,2,13,4,7,15,6,8,12,11,9,10,14,5,3	G_{14}	0,1,2,13,4,7,15,6,8,14,12,11,3,9,5,10
G_7	0,1,2,13,4,7,15,6,8,12,14,11,10,9,3,5	G_{15}	0,1,2,13,4,7,15,6,8,14,12,11,9,3,10,5

表 2 满足 $\deg(S_p)=2,3$ 的矢量 $p\in F_2^n\setminus\{0\}$ 的个数

Table 2 Number of $p\in F_2^n\setminus\{0\}$ such that $\deg(S_p)=2,3$

次数	S-Box 代数							
	G_0	G_1	G_2	G_3	G_4	G_5	G_6	G_7
$\deg(S_p)=2$	3	3	0	0	0	0	0	0
$\deg(S_p)=3$	12	12	15	15	15	15	15	15

次数	S-Box 代数							
	G_8	G_9	G_{10}	G_{11}	G_{12}	G_{13}	G_{14}	G_{15}
$\deg(S_p)=2$	3	1	1	0	0	0	1	1
$\deg(S_p)=3$	12	14	14	15	15	15	14	14

性质。

定义 3[27] 设有 r 轮 n 比特迭代分组密码，其轮函数为 $F_2^n\rightarrow F_2^n$。若 K 为轮密钥，则密钥异或的轮函数为 $F_K(x)=F(x\oplus K)$。为方便说明，本文忽略白化密钥，则明文 P 经算法到密文 C 的加密过程可以表示为：

$$x_0=P$$
$$x_{i+1}=F_{K_i}(x)=F(x\oplus K_i),(i=0,1,\cdots,r-1)$$
$$C=x_r$$

定义 4[27] 若有密钥 K 满足以下关于轮函数的非线性布尔函数 g：

$$g(F_K(x))=g(x\oplus K)\oplus c=g(x)\oplus g(K)\oplus c$$

其中 $c\in F_2$ 为常量，则称这些密钥为弱密钥(Weak Keys)，函数 g 称为轮函数的**非线性不变子**。

Todo 等人[27]指出，非线性不变子攻击的核心是寻找密码算法的非线性不变子。而 S 盒作为算法重要的非线性部件，由此该方法的关键在于寻找到 S 盒的输入输出的非线性不变子。即找到 n 比特 S 盒 $S(x):F_2^n\rightarrow F_2^n$ 输入输出的如下关系：

$$g(S_K(x))=g(x\oplus K)\oplus c=g(x)\oplus g(K)\oplus c$$

基于定义 3、4，Wei 等人[30]对非线性回路代数关系作了如下阐述：

定义 5[30] 对任意的 S 盒 $S(x):F_2^n\rightarrow F_2^m$，若满足

$$\begin{cases} f(x)\oplus g(S(x))=c_1 \\ f(S(x))\oplus g(x)=c_2 \end{cases}$$

其中： $f(x)$， $g(x)$ 为两个 m 元布尔函数， c_1， $c_2\in F_2$ 为常量。称该方程为 S 盒的**非线性回路代数关系**， $f(x)$， $g(x)$ 为 S 盒的非线性回路函数（简称回路函数）。S 盒非线性回路代数关系是使用非线性函数以概率 1 逼近 S 盒。令 $F(x,S(x)):F_2^m\rightarrow F_2=f(x)\oplus g(S(x))$，则定义 S 盒的回路函数集合为

$$U(F)=\{F(x,S(x))\,|\,f(x)\oplus g(S(x))=c_1,f(S(x))\oplus g(x)=c_2,x\in F_2^n\}$$

令 $V(x,S(x)):F_2^m \to F_2 = g_1(x)\oplus g_1(S(x))$，定义 S 盒的非线性不变子集合如下：

$$U(V)=\{V(x,S(x))|g_1(x)\oplus g_1(S(x))=c, x\in F_2^n\}$$

当 $f=g$ 时，则 f，g 为 S 盒的非线性不变子（简称不变子）。可以发现，在上述定义下，非线性不变子是回路代数关系的特殊形式，回路代数关系比非线性不变子更具一般化。观察到，S 盒的回路函数扩展至算法的轮函数也成立时，可以使用回路函数以概率 1 逼近算法，从而用于区分攻击。

2.2 非线性回路代数关系求解算法

下面简要介绍回路代数关系的求解算法：将回路代数关系方程使用布尔函数代数正规型形式展示有

$$\begin{cases}\sum\limits_{u\in F_2^n} a_u x^u \oplus \sum\limits_{u\in F_2^n} b_u S(x)^u = c_1 \\ \sum\limits_{u\in F_2^n} a_u S(x)^u \oplus \sum\limits_{u\in F_2^n} b_u x^u = c_2\end{cases}$$

其中，a_u，$b_u\in F_2$ 分别为回路代数关系函数 $f(x)$，$g(x)$ 的未知系数，$x^u=\Pi_{i=1}^N x_i^{u_i}$，由 n 比特 S 盒的输入输出确定的如上方程组共 2^n 个，方程总数为 2^{n+1} 个。为简单而不失一般化，首先介绍一种通用的分析方法：

算法 1　通用的 n 比特 S 盒回路代数关系求解算法

a)由于未知系数 a_i，$b_i\in F_2(0\le i\le u)$ 的取值范围已知，即任意比特系数取值非 0 即 1，令矢量 $A_u=(a_0,a_1,\cdots,a_u)$，$B_u=(b_0,b_1,\cdots,b_u)(w(u)=k)$，称 A_u，B_u 为系数矢量。每次按字典序各取一固定值的 A_u，$B_u(0<A_u,B_u\le 2^{C_n^1+C_n^2+\cdots+C_n^k}-1)$，通过限制 u 的汉明重为 k，来实现求解的回路代数关系的最高代数次数为 k。若 u 的汉明重为 n，则可求解出已知 S 盒的所有回路代数关系。

b)按顺序取输入对 $(x_0,S(x_0))$，$(x_0+1,S(x_0+1))$，求解相应的 $(x_0^u,S(x_0)^u)$，$((x_0+1)^u,S(x_0+1)^u)$，代入回路代数关系方程中求得常数组 (c_{1,x_0},c_{2,x_0}) 和 $(c_{1,x_0+1},c_{2,x_0+1})$。

c)判定 $F(x)$ 是否成立。若等式成立，则依字典序继续取值，直至遍历所有的输入对 $(x_0,S(x_0))(x_0\in F_2^n)$，使得判定等式均成立，存储此时的 $A_u=(a_0,a_1,\cdots,a_u)$，$B_u=(b_0,b_1,\cdots,b_u)$，c_1，c_2。即对所有的 $(x_0,S(x_0))$，均满足系数为 a_0，a_1，…，a_u，b_0，b_1，…，b_u 的闭环子方程，其中方程常数为 c_1，c_2；若等式不成立，则直接跳入步骤 d）。

d)改变 A_u 或 B_u 的值，重复步骤 b)c)，依次寻找符合条件的回路代数关系系数并将其保存。若 A_u，B_u 遍历完域 $F_2^{C_n^1+C_n^2+\cdots+C_n^k}$，则停止操作，至此得到全部最高代数次数为 k 的回路代数关系方程。

假设对 n 比特 S 盒求解代数次数为 k 的回路代数关系方程，则利用算法 1 求解，所需时间复杂度为 $O(2^{C_n^1+C_n^2+\cdots+C_n^k+n})$。可以看到，上述方法易于程序实现，能得到全部回路代数关系方程，但 n 值较大时，该方法效率相对较低。

下面，利用高斯消元求解思想介绍一种返回解集的基的方法。重写闭环不变子求解方程：

$$\begin{cases}\sum\limits_{u\in F_2^n} a_u x^u \oplus \sum\limits_{u\in F_2^n} b_u S(x)^u = c_1 & (1)\\ \sum\limits_{u\in F_2^n} a_u S(x)^u \oplus \sum\limits_{u\in F_2^n} b_u x^u = c_2 & (2)\end{cases}$$

方程 (1)⊕(2) 有

$$\sum_{u\in F_2^n}(a_u\oplus b_u)x^u \oplus \sum_{u\in F_2^n}(a_u\oplus b_u)S(x)^u = c_1\oplus c_2 \qquad (3)$$

此处令 $\delta_u=a_u\oplus b_u$，$C=c_1\oplus c_2$，则式(3)可写为

$$\sum_{u\in F_2^n}\delta_u(x^u\oplus S(x)^u)=C \qquad (4)$$

假设 u 的汉明重为 k，遍历 $x(x\in F_2^n)$ 的值代入方程 (4) 中，可得到方程个数为 2^n，变量个数为 $2*(C_n^1+C_n^2+\cdots+C_n^k)$ 的方程组，求解该方程组即可得到系数 δ_u。接下来，将 $b_u=a_u\oplus\delta_u$ 代入方程 (1) 或 (2)（此处以方程 (1) 为例）得到

$$\sum_{u\in F_2^n} a_u(x^u\oplus S(x)^u)\oplus\sum_{u\in F_2^n}\delta_u S(x)^u = c_1 \qquad (5)$$

同理，遍历 $x(x\in F_2^n)$ 值代入方程 (5) 中，求解方程组即可得到系数 a_u，最后利用 $b_u=a_u\oplus\delta_u$ 得到系数 b_u。该方法通过两次求解方程组，采取分而治之的方法，减少了每次求解的变量，降低了每次求解的时间复杂度（降至 $O(2^n+(C_n^1+C_n^2+\cdots+C_n^k)^3)$）和出错率，能快速高效求解回路代数关系方程。

3 一些 4 比特 S 盒的新分析

3.1 比特 S 盒回路代数关系求解算法的应用

由于 4 比特 S 盒数据复杂度较低，本节则利用回路代数关系求解的一般性方法，设计了求解程序，对 16 类最优 4 比特 S 盒及目前一些常用的轻量级 4 比特 S 盒进行了测试。

算法 2　计算 4 比特 S 盒回路代数关系的快速方法。

输入：4 比特 S 盒的输入 x、输出 $S(x)$。

输出：S 盒的闭环函数 $F(x)$、$G(y)$，常数 c_1、c_2。

a)给定 4 比特 S 盒 S-Box，定义向量 $X=(x_0,x_1,x_2,x_3)$，$Y=(y_0,y_1,y_2,y_3)\in F_2^4$，用于存储查表 S-Box 获得的数对 $(x,S(x))$。

b)定义一维数组 $X_u[15]$，$Y_u[15]$，数组元素 $X_u[i]$，$Y_u[i]\in F_2$。令 $u=(u_3,u_2,u_1,u_0)$ 的汉明重为 $w_u(1\le w_u\le 4)$，w_u 依次增大，u 的非零值由低位向高位过渡变化，计算固定 X，Y 值下的 X^u，Y^u，依次存储于数组 $X_u[15]$，$Y_u[15]$ 中。例如，$X_u[0,\cdots,3]=\{x_0,\cdots,x_3\}$，$u$ 分别取 $(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0)$。$X_u[4]=x_0x_1(u=(0,0,1,1))$，$X_u[5]=x_0x_2(u=(0,1,0,1))$，$X_u[6]=x_0x_3(u=(1,0,0,1))$，依此类推，$Y_u[15]$ 的存储与 $X_u[15]$ 相似。

c)假设所求的回路代数关系的代数次数为 $k(1\le k\le 4)$，定义项数为 $Num=C_4^1+C_4^2+\cdots+C_4^k$。定义系数向量 $AB(a_0,a_1,\cdots,a_{Num},b_0,b_1,\cdots,b_{Num})$，$A(a_0,a_1,\cdots,a_{Num})$，$B(b_0,b_1,\cdots,b_{Num})$，数组元素为所求回路代数关系系数 a_i，$b_i\in F_2$，固定 $AB=AB_0$，取对应位保存 $A=A_0$，$B=B_0$。

d) 取输入 X_0，计算 $C_{1(X_0)}=\bigoplus\limits_{(0\le i\le Num)}(Xu[i]\bullet a_i\oplus Yu[i]\bullet b_i)$，$C_{2(X_0)}=\bigoplus\limits_{(0\le i\le Num)}(Xu[i]\bullet b_i\oplus Yu[i]\bullet a_i)$；令 $X_0=X_0+1$，计算 $C_{1(X_0+1)}$，$C_{2(X_0+1)}$。若同时满足 $C_{1(X_0)}=C_{1(X_0+1)}$，$C_{2(X_0)}=C_{2(X_0+1)}$，则继续按字典序增大 X_0，重复 Step 4，直至遍历所有 X 取值，均满足上述条件，则保存此时的系数 A_0，B_0 及常数 C_1，C_2，闭环函数 $F(x)$ 的系数为 A_0，$G(y)$ 的系数为 B_0；否则，$AB=AB_0+1$，重复 Step 3~Step 4，直至遍历 F_2^{2Num} 域。

为了降低数据复杂度，提高回路代数关系函数的应用效率，利用算法 2 寻找了一些 4 比特 S 盒的二次回路代数关系，搜索结果整理如表 3 和 4 所示（表中“+”表示异或）。本文使用一台普通 PC 机进行实验，实验配置如表 5 所示。

3.2 16 类最优 4 比特 S 盒代表元二次代数关系分析

由表 3 可发现，16 类最优 4 比特 S 盒代表元中，，G_{15} 两个代表元的二次回路代数关系个数为 7 个，是 16 个代表元中二次回路代数关系总数最多的代表元，这些 S 盒存在潜在的安全缺陷。

3.3 常用轻量级 4 比特 S 盒二次代数关系分析

表 4 展示了常见的轻量级密码算法 4 比特 S 盒的二次非线性回路代数关系的搜索结果。经对比可以发现，非线性回路代数关系不同于差分均匀性和非线性度，该性质并不为仿射等价不变量。比方说，LBlock 算法的 10 个 S 盒均为 G_8 的

仿射等价类，但 10 个 S 盒的二次回路代数关系的形式及数量均有差异。

表 3　16 类最优 4 比特 S 盒 deg＝2 的回路代数关系统计表

Table 3　Loop algebraic relation of all 16 classes of optimal 4 bit S-boxes such that deg＝2

S 盒	二次回路代数关系示例（含不变子）	总数/个
G_0	$F(x)=x_0+x_1+x_3+x_0x_1+x_0x_3$ $G(y)=y_0+y_1+y_3+y_0y_1+y_0y_3$ $c_1=c_2=0$	7
G_1	$F(x)=x_0+x_1+x_3+x_0x_1+x_0x_3$ $G(y)=y_0+y_1+y_3+y_0y_1+y_0y_3$ $c_1=c_2=0$	3
G_2	/	无
G_3	$F(x)=x_2+x_0x_3+x_1x_3$ $G(y)=y_2+y_0y_3+y_1y_3$ $c_1=c_2=0$	1
G_4	$F(x)=x_0+x_1+x_3+x_0x_1+x_2x_3$ $G(y)=y_0+y_1+y_3+y_0y_1+y_2y_3$ $c_1=c_2=0$	3
G_5	$F(x)=x_0+x_1+x_3+x_0x_1+x_2x_3$ $G(y)=y_0+y_1+y_3+y_0y_1+y_2y_3$ $c_1=c_2=0$	3
G_6	$F(x)=x_0+x_1+x_3+x_0x_1+x_2x_3$ $G(y)=y_0+y_1+y_3+y_0y_1+y_2y_3$ $c_1=c_2=0$	1
G_7	$F(x)=x_0+x_1+x_3+x_0x_2+x_1x_2+x_2x_3$ $G(y)=y_0+y_1+y_3+y_0y_2+y_1y_2+y_2y_3$ $c_1=c_2=0$	3
G_8	/	无
G_9	$F(x)=x_0+x_1+x_3+x_0x_2+x_0x_3+x_1x_2+x_2x_3$ $G(y)=y_0+y_1+y_3+y_0y_2+y_0y_3+y_1y_2+y_2y_3$ $c_1=c_2=0$	1
G_{10}	$F(x)=x_0+x_3+x_0x_2+x_0x_3+x_1x_3+x_2x_3$ $G(y)=y_0+y_3+y_0y_2+y_0y_3+y_1y_3+y_2y_3$ $c_1=c_2=0$	1
G_{11}	$F(x)=x_0+x_1+x_3+x_0x_1+x_2x_3$ $G(y)=y_0+y_1+y_3+y_0y_1+y_2y_3$ $c_1=c_2=0$	1
G_{12}	$F(x)=x_0+x_1+x_2+x_3+x_0x_1+x_1x_3$ $G(y)=y_0+y_1+y_2+y_3+y_0y_1+y_1y_3$ $c_1=c_2=0$	7
G_{13}	/	无
G_{14}	$F(x)=x_0+x_1+x_3+x_0x_2+x_1x_2+x_2x_3$ $G(y)=y_0+y_1+y_3+y_0y_2+y_1y_2+y_2y_3$ $c_1=c_2=0$	1
G_{15}	$F(x)=x_1+x_2+x_3+x_0x_3+x_1x_2$ $G(y)=y_1+y_2+y_3+y_0y_3+y_1y_2$ $c_1=c_2=0$	7

S 盒 LBlock/S₂ 的二次回路代数关系有 $F(x)=x_2+x_1x_2+x_1x_3+x_2x_3$，$G(y)=y_2+y_1y_2+y_1y_3+y_2y_3$，S 盒 LBlock/S₅ 的二次回路代数关系为 $F(x)=x_2+x_1x_2+x_2x_3$，$G(y)=y_2+y_1y_2+y_2y_3$，其余 LBlock 的 S 盒却不存在二次非线性回路代数关系。特别的，TWINE，PRINCE，PRIDE，Midori64，SKINNY，Marvin 等算法的 S 盒均存在二次非线性回路代数关系。即对这些轻量级算法进行不变子攻击时，攻击者能以概率 1 获得关于 S 盒的等式：$F(x)+G(y)=c_1$，$F(y)+G(x)=c_2$。

表 4　常见 4 比特轻量级密码算法 S 盒 deg＝2 的回路代数关系表

Table 4　Loop algebraic relation of some famous lightweight 4 bit S-boxes such that deg＝2

S 盒	仿射等价类	二次回路代数关系示例（含不变子）	总数/个
PRESENT/LED/PHONTON	G_1	/	无
TWINE	G_3	$F(x)=x_1+x_2+x_0x_1+x_1x_3+x_2x_3$ $G(y)=y_1+y_2+y_0y_1+y_1y_3+y_2y_3$ $c_1=c_2=0$	1
LBlock/S₀	G_8	/	无
LBlock/S₁	G_8	/	无
LBlock/S₂	G_8	$F(x)=x_2+x_1x_2+x_1x_3+x_2x_3$ $G(y)=y_2+y_1y_2+y_1y_3+y_2y_3$ $c_1=c_2=0$	1
LBlock/S₃	G_8	/	无
LBlock/S₄	G_8	/	无
LBlock/S₅	G_8	$F(x)=x_2+x_1x_2+x_2x_3$ $G(y)=y_2+y_1y_2+y_2y_3$ $c_1=c_2=0$	1
LBlock/S₆	G_8	/	无
LBlock/S₇	G_8	/	无
LBlock/S₈	G_8	/	无
LBlock/S₉	G_8	/	无
Piccolo	G_8	/	无
PRINCE	G_{13}	$F(x)=x_0+x_2+x_3+x_0x_1+x_0x_3$ $G(y)=y_0+y_2+y_3+y_0y_1+y_0y_3$ $c_1=c_2=0$	1
RECTANGLE	G_1	/	无
PRIDE	G_8	$F(x)=x_0+x_1x_2$ $G(y)=y_2$ $c_1=c_2=0$	63
Midori64/MANTIS	G_1	$F(x)=x_0+x_1+x_3+x_0x_2$ $G(y)=y_0+y_2$ $c_1=c_2=1$	63
SKINNY	G_8	$F(x)=x_1x_3$ $G(y)=y_0y_2$ $c_1=c_2=0$	3
Marvin	G_{13}	$F(x)=x_0+x_3+x_1x_3$ $G(y)=y_1+y_2$ $c_1=c_2=0$	7
Serpent/S₀	G_2	/	无
Serpent/S₁	G_0	$F(x)=x_0x_1+x_1x_3$ $G(y)=y_0y_1+y_1y_3$ $c_1=c_2=0$	1
Serpent/S₂	G_1	/	无
Serpent/S₃	G_9	/	无
Serpent/S₄	G_{14}	/	无
Serpent/S₅	G_{14}	/	无
Serpent/S₆	G_1	/	无
Serpent/S₇	G_9	/	无
GIFT	非最优 S 盒	/	无

表 5　计算机配置

Table 5　Computer configuration

名称	性能
CPU	Inter(R) Core(TM) i5-3230M
CPU 主频	2.60GHz
内存	16.0GB
系统类型	64 位 Windows 操作系统
编程软件	Microsoft Visual Studio 2010、Python 2.7

注意到，SKINNY，PRIDE，Midori64，MANTIS，Marvin 等算法 S 盒二次回路代数关系中二次项较少，甚至有线性回路代数关系，即算法存在潜在的安全缺陷。

根据表 4 可知，PRIDE S 盒的非线性二次回路代数关系共 63 个，比如：$F_S(x)=x_0\oplus x_1\oplus x_1x_2\oplus x_2x_3$，$G_S(y)=y_2\oplus y_3$，$G_S(y)$ 为线性函数。值得注意的是，Marvin 的 S 盒存在 7 个二次非线性回路代数关系，如下 S 盒回路代数关系 $F_S(x)=x_0\oplus x_3\oplus x_1x_3$，$G_S(y)=y_1\oplus y_2$，$F_S(x)$ 只有一个二次项，$G_S(y)$ 为线性函数，此回路代数关系既满足了非线性，又使得二次项数最少。

4　结束语

本文根据 S 盒的输入输出关系，将非线性回路代数关系应用于 4 比特 S 盒的性质研究，为 4 比特 S 盒的设计和分析提供了新的测试方法。本文设计了非线性回路代数关系的求解算法，主要应用于 16 类最优 4 比特 S 盒和一些常用的轻量级 4 比特 S 盒的测试。结果表明：16 类最优 4 比特 S 盒的代表元只有三类不存在回路代数关系；TWINE，PRINCE，PRIDE，Midori64，MANTIS，SKINNY，Marvin 等轻量级算法的 S 盒均存在不同数量的回路代数关系，为算法攻击提供了更多的可能性。

参考文献：

[1] Feistel H. Block cipher cryptographic system: US，Patent 3 798359 [P]. 1974-3-19.

[2] Weik M.H. Data encryption standard[C]//Computer Science and Communications Dictionary. Boston:Springer, 2000.

[3] Rijmen V, Daemen J. Advanced encryption standard [C]//Proc of Federal Information Processing Standards Publications, National Institute of Standards and Technology, 2001: 19-22.

[4] Leander G, Poschmann A. On the classification of 4 bit s-boxes [C]//Arithmetic of Finite Fields. 2007: 159-176.

[5] Anderson R. Serpent: a proposal for the advanced encryption standard [C]//Proc of the1st Advanced Encryption Standard (AES) Candidate Conference.1998: 83-87.

[6] Daemen J, Peeters M, Van G, *et al.* Nessie proposal: the block cipher Noekeon [J]. Nessie Submission, 2000.

[7] Cheng Lin, Zhang Wentao, Xiang Zejun. A new cryptographic analysis of 4-bit s-boxes [J]. Information Security and Cryptology,2015: 144-164.

[8] Bogdanov A, *et al.* Present: an ultra-lightweight block cipher[C]//Proc of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2007: 450-466.

[9] Knudsen L, Leander G, Poschmann A. Printcipher: a block cipher for ic-printing[C]//Cryptographic Hardware and Embedded Systems. 2010: 16-32.

[10] Guo Jian, Peyrin T, Poschmann A. The led block cipher[C]//Cryptographic Hardware and Embedded Systems.2011: 326-341.

[11] Wu Wenling, Zhang Lei. Lblock: a lightweight block cipher [C]//Applied Cryptography and Network Security.2011: 327-344.

[12] Borghoff J, *et al.* Prince-a low-latency block cipher for pervasive computing applications[C]//Advances in Cryptology-ASIACRYPT. 2012: 208-225.

[13] Beaulieu R, Treatman-Clark S, Shors D, *et al.* The SIMON and SPECK lightweight block ciphers [C]//Proc of the 52nd ACM/EDAC/IEEE Design Automation Conference. 2015: 1-6.

[14] Zhang Wentao, Bao Zhenzhen, Lin Dongdai, *et al.* Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms [J]. Science China Information Sciences, 2015, 58(12): 1-15.

[15] Albrecht R, Driessen B, Kavun B, *et al.* Block ciphers – focus on the linear layer (feat. pride) [C]//Advances in Cryptology-CRYPTO.2014: 57-76.

[16] Beierle C, *et al.* The skinny family of block ciphers and its low-latency variant mantis[C]//Advances in Cryptology-ASIACRYPT.2016: 123-153.

[17] Banik S, Pandey S, Peyrin T, *et al.* Gift: A small present[C]//Cryptographic Hardware and Embedded Systems.2017: 321-345.

[18] Bansod G, Patil A, Pisharoty N. Granule: an ultra lightweight cipher design for embedded security [J]. International IACR Cryptology ePrint Archive, 2018, 2018: 600.

[19] Saha S, Rarhi K, Bhattacharya A. Systematization of a 256-bit lightweight block cipher marvin [J]. Social Science Electronic Publishing, 2018.

[20] Guo Jian, Peyrin T, Poschmann A. The photon family of lightweight hash functions[C]//Advances in Cryptology-CRYPTO.2011: 222-239.

[21] Bogdanov A, Knežević M, Leander G, *et al.* Spongent: a lightweight hash function[C]//Cryptographic Hardware and Embedded Systems. 2011: 312-325.

[22] 吴文玲，冯登国，张文涛. 分组密码的设计与分析 [M]. 北京：清华大学出版社，2009. (Wu Wenling, Feng Dengguo, Zhang Wentao. Design and analysis of block ciphers [M]. Beijing: Tsinghua University Press, 2009.)

[23] 李超，孙兵，李瑞林. 分组密码的攻击方法与实例分析 [M]. 北京：科学出版社，2010. (Li Chao, Sun Bing, Li Ruilin. Attack method and case analysis of block cipher [M]. Beijing: Science China Press, 2010.)

[24] Saarinen M J O. Cryptographic analysis of all 4×4-bit s-boxes [C]// Proc of International Workshop on SAC. Berlin: Springer,2011: 118-133.

[25] Ullrich M, De Canniere C, Indesteege S, *et al.* Finding optimal bitsliced implementations of 4× 4-bit S-boxes [C]//Proc of Symmetric Key Encryption Workshop. 2011: 16-17.

[26] Zhang Wentao, Bao Zhenzhen, Rijmen V, *et al.* A new classification of 4-bit optimal s-boxes and its application to present, rectangle and spongent[C]//Fast Software Encryption. 2015: 494-515.

[27] Todo Y, Leander G, Sasaki Y. Nonlinear invariant attack–practical attack on full scream, iscream and Midori64. Cryptology ePrint Archive, Report 2016/732 [R/OL]. 2016. http://eprint. iacr. org/2016/732.

[28] Banik S. Midori: a block cipher for low energy[C]//Advances in Cryptology-ASIACRYPT. 2015: 411-436.

[29] Beierle C, Canteaut A, Leander G, *et al.* Proving resistance against invariant attacks: how to choose the round constants[C]//Advances in Cryptology-CRYPTO.2017: 647-678.

[30] Wei Yongzhuang, Ye Tao, Enes P, *et al*. Generalized nonlinear invariant attack and a new design criterion for round constants [J]. IACR Trans on Symmetric Cryptology,2018,2018(4):62-79.

[31] Tim B. Block cipher invariants as eigenvectors of correlation matrices Cryptology ePrint Archive, Report 2018/763[R]. 2018. http://eprint. iacr. org/2018/763.

[32] Shannon C. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[33] 温巧燕，钮心忻，杨义先. 现代密码学中的布尔函数 [M]. 北京：科学出版社，2000. (Wen Qiaoyan, Niu Xinxin, Yang Yixian. Boolean functions in modern cryptography [M]. Beijing: Science China Press, 2000.)

[34] Rothaus O. On"bent"functions [J]. Journal of Combinatorial Theory, Series A, 1976, 20(3): 300-305.

[35] 冯登国. 频谱理论及其在通信保密技术中的应用 [D]. 西安:西安电子科技大学, 1995. (Feng Dengguo. Spectrum theory and its application in communication security technology [J]. Xi'an:Xidian University, 1995.)

[36] Matsui M. Linear cryptanalysis method for DES cipher [C]//Advances in Cryptology-EUROCRYPT/ 1993, 765: 386-397.

[37] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems [C]//Advances in Cryptology-CRYPTO. 1990: 2-21.

[38] Nyberg K. Differentially uniform mappings for cryptography[C]//Advances in Cryptology-EUROCRYPT.1993: 55-64.

[39] Carlet C, Charpin P, Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems [J]. Designs, Codes and Cryptography, 1998, 15(2): 125-156.